מבוא להגנת סייבר:

אַבְטָחַת מֵידָע (**information security**) היא הענף העוסק בהגנה מפני גישה, שימוש, חשיפה, ציתות, שיבוש, העתקה או השמדה של מידע ומערכות מידע מצד גורמים שאינם מורשים או זדוניים ולספק סודיות, שלמות וזמינות של המידע ללא תלות בסוג המידע או בצורת האחסון, פיזית או אלקטרונית.

מערכות מידע עומדות בפני סיכונים יומיומיים המאיימים על שלמותן וביטחונן. ההגנה עליהן כוללת מספר רבדים, אבטחה פיזית של המבנה שבו נמצאות מערכות המחשב, אבטחה של מערכות החומרה והתוכנה, אבטחת רכיבי התקשורת ואבטחת המידע הנאגר בהן. מאגרי מידע רבים המשמשים יחידים, תאגידים ומדינות, מאוחסנים על גבי מחשבים בעלי גישה לאינטרנט. גם למאגר המבודל מהאינטרנט ניתן לגרום נזק באמצעות גישה ישירה. מאגרי מידע אלו כוללים מידע אישי, עסקי וביטחוני.

שלושת היעדים העיקריים של אבטחת מידע הם:

- **שלמות** (integrity). הגנה מפני שינוי זדוני של המידע או השמדתו, כולל הבטחת אי התכחשות ואימות זהויות בעלי המידע.
- **סודיות** (confidentiality). הגבלת גישה או חשיפה, כולל הגנה על פרטיות וזכויות קניניות.
- **זמינות** (availability). שמירה על זמינות ויעילות הגישה אל המידע בכל זמן נתון.

שלושה מרכיבים שונים הגורמים לסיכון:

1. **טכנולוגיות** – מערכות החומרה, התוכנה והתקשורת המהוות "מערכות";
2. **אנשים** – המשתמשים בטכנולוגיות, ולכן מהווים חוליה חלשה במיוחד, מכיוון שהם מפעילים או משתמשים בטכנולוגיות, ונוטים לעשות שגיאות המייצרות פרצות במערך ההגנה אשר מאפשרות לתוקף לנצלן.
3. **תהליכים** – מידת הנזק משגיאת אנוש או נקודת תורפה טכנולוגית עשויה לְהצטמצם מאוד אם מבוצע תכנון נכון של התהליכים בארגון. הגדרת תהליכים בסדר נכון ובדוק מראש מאפשרת זיהוי מוקדם של פגיעה או ניסיון פגיעה במערכות.

אבטחה לעומת נוחות

ישנו ניגוד מתמיד בתהליך קבלת ההחלטות מצד המשתמשים בין אבטחה מול נוחות. הדרך העיקרית להשגת אבטחה מלאה היא ניתוק המערכת מהרשת, הסרת חיבור הרשת, המקלדת, העכבר, הצג, כונן התקליטונים והמדפסת, אך הדבר אינו מעשי וגם לא תמיד מספיק כיוון שתמיד קיים חשש שגורמים עוינים יצליחו להשיג גישה פיזית כמו החדרת דיסק און קי נגוע. הרעיון המרכזי באבטחה הוא שככל שהגישה למחשב נרחבת יותר, כך הוא פחות מאובטח. מנגד, הדרך הנוחה ביותר להשתמש במחשב היא להופכו לזמין מכל מקום בעולם, להשתמש בכל פרוטוקולי התקשורת הקיימים וללא סיסמאות, במקרה כזה רמת האבטחה שואפת לאפס.

ככל שהאמצעי ההגנה פוגעים יותר בנוחות השימוש יש סיכוי גדול יותר שהמשתמשים ינסו לעקוף או לנטרל אותם. למשל ידוע שמשתמשים נוטים לבחור בסיסמאות חלשות וקשה לאכוף כללים קפדניים שמונעים זאת. לכן חשוב לאזן בין הפגיעה בנוחות השימוש לבין אמצעי האבטחה המופעלים.

נזקי אובדן אמון לקוחות

בעיה נוספת העולה מתקיפת מערכות מידע של חברות היא אובדן אמון הלקוחות בחברה. במערכות המידע של חברות רבות מצויים מאגרי מידע המכילים פרטים המשויכים לקהל הלקוחות, וכאשר גורמים שאינם מורשים מפלסים דרך גישה למאגרים אלו, הופכים קהל לקוחותיה גם הם לקורבן. במקרה שהדבר מתפרסם ונודע ללקוחות, צפוי נזק רב לחברה, ובשל כך חברות רבות אינן מדווחות על כשלי אבטחה במערכת שלהן, על מנת להימנע ממבוכה ציבורית ופגיעה בשמן הטוב ובאמון הלקוחות.

סוגי האקרים:

כובע לבן

האקר בעל כובע לבן הוא מי שמשתמש בידיעותיו במחשבים כדי לבדוק יציבות של תוכנות, מחשבים או רשתות ואת עוצמת המיגון שלהם. האקרים של כובע לבן פעמים רבות עובדים בתחום אבטחת המחשבים, ונחשבים חלק מן הממסד. הם גם מכונים Ethical Hackers - "האקרים מוסריים".

גם האקרים שאינם מועסקים בתחום ומאתרים פרצות אבטחה ללא תיאום מראש, אך ברגע שמתגלית הפרצה הם מדווחים עליה לבעלי האתר, רואים בעצמם האקרים של כובע לבן, על אף שצורת פעולה שכזו פחות ממוסדת ומתאימה לאחת ההגדרות ל"כובע אפור".

המאפיין העיקרי של האקרי כובע לבן הוא המניע שלהם - שיפור האבטחה של הקורבן.

מעצם עיסוקם באבטחה, האקרים של כובע לבן לרוב רואים בהאקרים של כובע שחור גורם מזיק ומטריד.

כובע שחור

האקר של כובע שחור הוא מי שמשתמש בידיעותיו במחשבים כדי להפיל או לחדור למערכות ללא רשות ולדלות משם פרטים או לשנות דברים. לרוב פעולתיו ייחשבו עבירה על החוק. כאשר האקר של כובע שחור מוצא פרצה סביר להניח שהוא ישתמש בה לצרכיו, ובמקרים אחרים אולי אף יסחור בה.

האקר כובע שחור לרוב מאופיין בכך שהוא אינו מעוניין בטובתו של הקורבן. לפיכך פעולותיהם של הכובעים השחורים מאופיינים יותר בגניבת מידע ובגרימת נזק למערכות או לשירותים. שימוש בכלים כגון שתילת סוס טרויאני, שתילת וירוסים ותולעת המחשבים.

האקרים יכולים לבחור להיות כובע שחור מסיבות רבות. ישנם בעלי אידאולוגיה אנטי ממסדית, אשר רואים בכובעים הלבנים את נציגי הממסד שמשמשים להגביל את החופש של האזרח, וגאים להיות כובעים שחורים. למשל, ב–2011, כשהנשיא חוסני מובארק ניסה לנתק את מצרים מהאינטרנט, האקרים עזרו למוחים במצרים להתחבר.

אולם, ישנם גם מי שפועלים ככובעים שחורים מסיבות של חמדנות גרידא - הם משמשים "שכירי חרב טכנולוגיים" לגורמים פליליים, או שהם עצמם עוסקים בפלילים למטרות רווח. וישנן עוד סיבות רבות ומגוונות. המושג משמש גם בהקשר של קידום אתרים (קידום כובע שחור) לתיאור מקדם שפועל בשיטות שאינן אתיות או שאינן חוקיות.

כובע אפור

האקר של כובע אפור הוא מי שמשתמש בידיעותיו במחשבים כדי לחקור ולחפש ידע נוסף בתחום, או מי שכוונתו לא בהכרח ברורה. הוא אינו מעוניין לגרום נזק לקורבן, אך גם לא מעוניין לסייע לו.
הגדרה אחרת מגדירה את האקר הכובע האפור בתור מי שמערב גישות של כובע שחור וכובע לבן, ואינו עקבי באחת מגישות אלו.
האקרים של כובע אפור הרבה פעמים יהיו אדישים לטובתו של הקורבן, מטרתם היא לרוב למידת הטכנולוגיות והאתגר של ההתנסות בהן.
למעשה הגדרת הכובע האפור נועדה לאפשר את תחום הביניים שבין הלבן המובהק לשחור המובהק.

מעט סיפורים מפורסמים בנושא מתקפות סייבר:

בשנת 2010 התגלתה מתקפת סייבר מתוחכמת במיוחד שנקראה סטקסנט. ככל הידוע, זו הפעם הראשונה שבה נחשף מהלך מדינתי רחב היקף שתכליתו לפגוע בעולם הפיזי של תשתיות קריטיות במדינת יעד ובמקרה הזה, בצנטריפוגות להעשרת אוראניום של איראן. הערכה היא כי הנוזקה הייתה כבר הייתה פעילה משנת 2007. בספטמבר 2011 התגלתה נוזקה בעלת מאפיינים דומים שכונתה דוקו.

בנובמבר 2014, התנהלה מתקפת ההאקרים על סרטי סוני. מבצע זה כלל גניבה מסיבית של פרטי לקוחות, גניבה רחבת היקף של סרטים שטרם הופצו לקהל הרחב, גניבה רחבת היקף של דוא"לים פנימיים ושימוש בנוזקות שמוחקות דיסקים פיזית.[10] חלק מהחוקרים מאמינים כי תקיפה זו מתבצעת על ידי "תוקפים מדינתיים" מקוריאה הצפונית, שמטרתם לפגוע בחברת סוני מכיוון שהיה בכוונתה לפרסם סרט שבראיית המשטר של קוריאה הצפונית, הוא פוגעני כלפיהם.[11][12]

במהלך מאי 2015, המגזין המקוון Wired פרסם צו החרמת ציוד מחשבים של ה-FBI כנגד אדם בשם כריס רוברטס. אותו כריס, מי שהיה מומחה אבטחה של אחת מחברות התעופה ופוטר, טוען שבמשך כחמש שנים, מ-2011 ועד 2014, הוא הצליח להתחבר לרשתות המיחשוב של מטוסי נוסעים, באוויר, בהיותו ישוב בתא הנוסעים

ודרך חיבור זה - לגרום לאווירון לתופעות לא מתוכננות שונות ובכלל זה, האצה של מנוע. הדעות חלוקות לגבי השאלה האם אמנם הוא ביצע את מה שהוא אמר או שמדובר בהונאה. התצהיר שהוגש מופיע באותה כתבה ב-Wired.[16] גם בעברית פורסמו מספר כתבות בנושא[17]

עובד קבלן של ה-NSA האמריקאית בשם אדוארד סנודן החל להדליף בצורה שיטתית, פרטים על כלים ושיטת פעולה של הסוכנות ובכלל זה עבודה בשיתוף פעולה עם חלק מהחברות העולמיות בתחום האינטרנט (כולל גוגל, אפל ורבות נוספות), תקיפות סייבר לאיסוף מידע על ממשלות ותאגידים בכל העולם, כולל על מדינות ידידותיות לארצות הברית כמו גרמניה וישראל, קיומן של יחידות טכנולוגיות ממגוון סוגים וקיומה של יחידה שמתמחה ביצירת דרכי גישה לרשתות ומחשבים בשם Tailored Access Operations.[20][21]

במהלך השנים 2015–2016, בוצעה התקפה על מחשבי ה"וועידה הדמוקרטית הלאומית", בארצות הברית. האתר ויקיליקס פרסם כמות גדולה של מסמכי דוא"ל ממחשבי פוליטיקאים דמוקרטים, שנגנבו במהלך אותה תקיפה מדוברת. רבים ייחסו את התקיפה לרוסיה, כולל נשיא ארצות הברית בנאום פומבי. וראו בזאת ניסיון להתערבות רוסיה בבחירות לנשיאות ארצות הברית ב-2016.[25]

במהלך מרץ 2018, עיריית אטלנטה בארצות הברית נתקפה באמצעות "קריפטולוקר". עיריית אטלנטה משרתת כשישה מיליון אזרחים. ההתקפה גרמה לכך שלא ניתן לשלם קנסות חניה לעירייה, אי אפשר להסדיר תשלומי מים, לא ניתן לגשת לארכיון בתי המשפט, לשוטרים אין גישה לבסיסי הנתונים של המשטרה, למבקרת העירייה - אין גישה לקבצים שלה, האזרחים לא יכולים "לפתוח קריאה" לטיפול בבורות בכביש, מפגעי רעש, גרפיטי או נושאים הקשורים לפינוי אשפה.[37]

לפי פורבס, Wired ואתרים נוספים, במסגרת הלחימה של ישראל ברצועת עזה, במהלך מאי 2019 - אנשי החמאס יזמו מתקפת סייבר נגד ישראל וכתגובה, ישראל השמידה את הבניין ממנו הם פעלו. אם זה נכון, זה האירוע הידוע הראשון בהיסטוריה שבו מדינה תוקפת תקיפה פיזית, קינטית - את מי שתקף אותה תקיפת סייבר.[69]

ב-26 ביולי 2019 התפרסם כי אחת מחברות החשמל הגדולות בדרום אפריקה, הותקפה באמצעות "קריפטולוקר". המתקפה גרמה לחוסר יכולת לגשת לבסיסי הנתונים, לחוסר יכולת לתפעל אפליקציות ולפגיעה מסיבית ברשתות החברה בכלל. כתוצאה מהתקיפה, החברה הפסיקה לספק חשמל לצרכניה.[83]

מקור:
https://he.wikipedia.org/wiki/%D7%9E%D7%AA%D7%A7%D7%A4%D7%95%D7%AA_%D7%A1%D7%99%D7%99%D7%91%D7%A8

אימות זהות:

באבטחת מידע וקריפטוגרפיה, **אימות** (באנגלית: Authentication) מתייחס לפעולה שנועדה לאשר תקפות פיסת מידע שישות כלשהי טוענת לאמיתותה.

בניגוד לזיהוי, שמתייחס להצהרה באשר לזהותו של אדם או ישות כלשהי באמצעות חפץ או טענה, כדי למנוע התחזות, האימות הוא בעצם התהליך שבאמצעותו מוודאים את נכונות ואמיתות הטענה.

האימות כרוך לרוב בצורה אחת או יותר של אמצעי זיהוי כמו תעודה מזהה, בדיקת הרשאה או בדיקת אותנטיות אתר אינטרנט באמצעות תעודת מפתח ציבורי.

אימות מתחלק לשלוש קטגוריות עיקריות:

1. **ידיעה**. משהו שהטוען **יודע** (כגון סיסמה, מספר זיהוי אישי או מענה על אתגר).
2. **שייכות**. משהו ברשותו או בבעלותו של הטוען (כגון תעודה מזהה, כרטיס מגנטי, אסימון אבטחה המוטמע במכשיר נייד או טלפון נייד עליו מותקן יישומון אבטחה).
3. **זהות**. תכונה פיזית של הטוען (כמו חתימת יד, טביעת אצבע, זיהוי ביומטרי כמו זיהוי פנים, סריקת רשתית או דגימת DNA).

כאשר נחוץ אימות ברמת ודאות יותר גבוהה, נעשה שימוש באימות דו-שלבי או אימות רב-שלבי שבו משלבים מספר אמצעי אימות השייכים לשתים או יותר מהקטגוריות המנויות. כמו אימות דו שלבי של גוגל שכאשר מופעל דורש מהמשתמש להקליד סיסמה (קטגוריה ראשונה) ולהפגין ידיעת מספר אקראי שנוצר באמצעות אפליקציית אבטחה (קטגוריה שנייה).

פעולת אימות אלקטרונית שמתבצעת בהיקף רחב החל מהרבע האחרון של המאה העשרים היא זו המשמשת למשיכת כספים ממכשיר בנק אוטומטי. לזיהוי המושך משמש שילוב של שני אמצעים: כרטיס מגנטי שעליו מוטבע זיהוי של המושך, והקשה של סיסמה הידועה רק למושך. גניבה של רק אחד משני אמצעים אלה אינה מאפשרת התחזות.

במקרים שפעולת האימות היא פחות קריטית, נהוג להסתפק באמצעי זיהוי אחד בלבד. בשעון נוכחות די, בדרך כלל, בהעברת הכרטיס המגנטי, ואין צורך ללוות זאת בסיסמה. בכניסה לאתרי אינטרנט רבים, ובכלל זה ויקיפדיה, די בהקלדת זיהוי משתמש וסיסמה, ואין צורך באמצעי זיהוי פיזי.

כרטיס מגנטי הוא אמצעי אבטחה נפוץ, אך ניתן לזייפו. כאשר נחוץ זיהוי ברמת ודאות גבוהה, ניתן להחליף את הכרטיס המגנטי בזיהוי ביומטרי, שאותו קשה יותר לזייף. זיהוי ביומטרי הוא זיהוי על-פי תכונות ביולוגיות של המשתמש, כגון טביעת אצבע, סריקת רשתית או בדיקת דנ"א.